CWIN | Critical infrastructure Warning Information Network

CWIN*Report*

Fall 2004

Vol. II, No. 3

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

In This Issue

Keeping the Network Secure

A Round Table Discussion

The Critical infrastructure Warning Information Network's (CWIN) data and voice traffic ride across a protected network backbone managed by National Communication System (NCS) contractor Arrowhead Global Solutions. Network services are provided under subcontract by AT&T Government Solutions. The CWIN Report editor sat down with NCS/CWIN program manager Kevin Piekarski, Arrowhead Vice President of Information Technology Gus Tome and AT&T security chief Ed Amoroso to talk about network security.

Editor: Describe the underlying assumptions that drove the CWIN architecture design.

Piekarski: NCS mandated that CWIN be a high performance network, always available, regardless of the state of the public switched network or the public Internet. Further, NCS demanded a

continued on page 2

CWIN Moves to Infrastructure Coordination Division

The National Communications System (NCS) started transitioning the Critical infrastructure Warning Information Network (CWIN) program to the Infrastructure Coordination Division (ICD) in early August. ICD, directed by Jim Caverly, falls within the Department of Homeland Security under the Information Analysis and Infrastructure Protection Directorate (IAIP). ICD acts as the hub of infrastructure expertise for IAIP by sustaining core

continued on page 4

DHS Provides States Critical Link

The Department of Homeland Security (DHS) began steps in early August to expand Critical infrastructure Warning Information Network (CWIN) membership to the 50 States and Washington, DC, ensuring nationwide coverage for this critical information network. DHS will deploy CWIN terminals to the state homeland security offices to provide reliable and protected connectivity between the Federal Government, private sector and states. DHS announced the initiative through several conference calls held between DHS and the state homeland security offices on August 5.

Generation Next

The National Communication System (NCS) is in the process of updating the thin client workstations that NCS originally provided. A second generation Critical infrastructure Warning Information Network (CWIN) workstation is now available, and we'll be deploying it to current CWIN user sites over the next few months.

What can you expect from your new unit? A state-of-the-art NYTOR thin client, which offers 1024 MB RAM and comes complete with a Pentium 1000, is replacing the original client. We upgraded the flat-screen monitor display from 15 to 17 inches. You will also receive an optical mouse and an enhanced keyboard equipped with a smart card reader. Smart card implementation, which will allow more secure network logon, will take place this fall; you'll receive additional information on this later. The new client also includes Adobe Acrobat Reader.

NCS will deploy the second generation workstations over the next three months. You'll receive a phone call before your equipment ships, and soon thereafter you can expect packages in the mail. We'll provide new user manuals via CD and the CWIN intranet, but your shipment will include a step-by-step setup guide to get you started. Additionally, a CWIN technician will assist you with your installation via telephone.

You'll also be getting directions for returning the old equipment, including boxes, packaging instructions, postage and a mailing address. Please return your first generation unit as soon as you install the new one.

After you have a chance to familiarize yourself with the new workstation, please feel free to provide any comments or feedback you may have.

Keeping Secure *continued from page 1*

flexible network, able to readily expand to include new members regardless of geographic location. Finally, security is critical; network integrity must be maintained at all times.

Editor: Is CWIN riding on its own dedicated pipe?

Tome: Yes and no. In the magic of today's digital world, where network architects can capitalize on both physical and logical means to design networks, CWIN uses a hybrid network topology. This extremely sophisticated network uses multi-protocol label switching (MPLS) in a virtual private network (VPN), providing reliability, scalability and security. MPLS/VPN is a next generation networking protocol that offers increased efficiency, reliable data transport and sender identity assurance. The combination of these features provides CWIN with an extraordinary level of data security.

Editor: Can you describe that network a little more so we have a clearer understanding of its security aspects?

Amoroso: If NCS had designed CWIN only a few years ago, the logical choice would have been a frame relay network. However, in the last several years, we've developed various new network technologies that take advantage of improvements in networking and protocols. For example, CWIN combines the data link layer 2 access with a layer 3 network core that replaces traditional frame relay backhaul.

The network that supports CWIN is both physically isolated and operationally partitioned from the Internet. The Internet edges and CWIN edges are on different physical routers, resulting in physical isolation. CWIN is on the IP-enabled layer 2 network, with the Internet running on top of the separate "True IP" layer 3 network to provide operational partitioning.

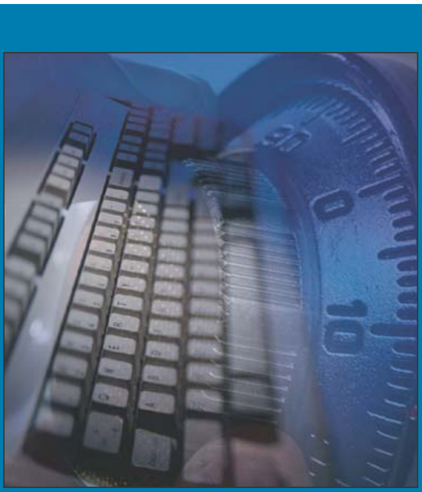
Editor: Well, how does AT&T make sure that CWIN traffic doesn't become infected from Internet virus attacks or any of the other vulnerabilities that afflict modern computers?

Amoroso: In cases where the traffic is distributed over the nationwide fiber backbone, the two types of

Security Lock-down:

Packet Protector

Cary Riddock
Security Consultant



The Internet is a great business asset, but despite the best efforts of virus protection programs, it's not a very secure place to communicate. Trojan horses, spyware, cookies... the list of intrusive agents on the Web abounds. Illegitimate packet sniffing is one threat that often sneaks under our cyber security radar.

While packet sniffers are an honest means of network maintenance in the hands of honest administrators, the "bad guys" know about this technology as well, and they can use the tool for illegitimate purposes.

For those unfamiliar with the concept, packet sniffers are programs that observe network traffic. Much like wiretaps allow the FBI to eavesdrop on telephone conversations, packet sniffers enable both legitimate as well as unauthorized parties the ability to "listen in" on network communication.

How do they achieve this? On a private network, all computers attach to the same common backbone or network segment. Ordinarily, your computer can only see traffic that has been specifically addressed to it. A packet sniffer allows that same computer to see all the traffic being transmitted on the network, regardless of destination. If properly equipped, the packet sniffer can also record traffic for later perusal.

So, how do packet sniffers affect the Critical infrastructure Warning Information Network (CWIN)? That's the good news – they don't. CWIN is physically isolated and operationally partitioned from the Internet, and it uses a hybrid network infrastructure. Users connect on the data link layer, and from there traffic is handed off to the network layer in the form of packets. The packets are parceled in multi-protocol label switching (MPLS) labels, which dictate prearranged paths through the system. The network layer always remains hidden from the user.

Aside from the hybrid infrastructure, CWIN employs MPLS/Virtual Private Network (VPN) technology that provides additional data security. While a traditional Ethernet-connected system allows all Internet protocol-enabled devices to insert packets into the network with any source and destination address, CWIN only accepts recognized user packets.

In a perfect world, all networks would be invulnerable to cyber attack. But it's not a perfect world, and there are real hazards lurking in cyberspace. Packet sniffers are one such hazard, but fortunately, they have no effect on CWIN.

Mr. Riddock provides network security consulting services for Arrowhead Global Solutions, under contract to the NCS.

traffic run over physically independent network infrastructures. The only way for Internet traffic to intrude upon CWIN is through extensive modification to the routing and forwarding tables that provide the addressing for each packet.

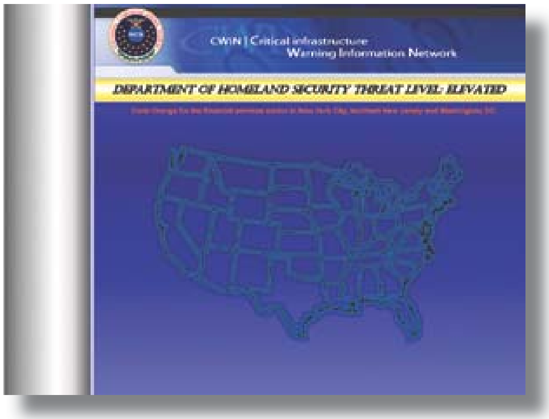
Additionally, Quality of Service (QoS) is implemented to ensure that varying types of traffic do not overwhelm the capabilities of the data circuit. QoS allows applications and users to request and receive a predictable level of service for each traffic type. This focus achieves predictability, reliability and availability in the network by keeping the intelligence at the network edges since this is where most problems (congestion) occur, and therefore minimizes complexity in the backbone.

Piekarski: We'd like the CWIN community to understand that the backbone network combines the robustness of the public network with the security required for sensitive communications infrastructures. The backbone offers the security

continued on page 4

CWIN to Offer Active Desktop

Critical infrastructure Warning Information Network (CWIN) users noticed a change to the CWIN desktop a few weeks ago: Department of Homeland Security (DHS) began to make it an active desktop. Active desktop integrates the desktop feature with Internet Explorer browsing software to provide access to information using the browser application.



CWIN | Critical infrastructure Warning Information Network

DEPARTMENT OF HOMELAND SECURITY THREAT LEVEL: ELEVATED

To improve the network's functionality, CWIN is moving toward the introduction of a more active desktop tailored to meet the requirements of the different critical infrastructure sectors. Earlier this summer, CWIN began publishing the DHS alert notice. In August, when DHS raised the alert for the financial sector in New York, New Jersey and Washington, DC, CWIN posted that information as well.

Look for more improvements later this year!

***CWIN to ICD** continued from page 1*

sector expertise, maintaining operational awareness and fostering working-level relationships with Federal Agencies, industry and State and local government. ICD works with all the infrastructure sectors and develops shared tools and watch and warning capabilities to maintain operational awareness. CWIN is an effective tool supporting ICD in its mission.

***Keeping Secure** continued from page 3*

of a private point-to-point network without the accompanying costs and inflexibility of such a network. Operating 24x7, CWIN is always available for communicating important alerts and advisories, sharing information and working with Government and other partners both within and among the critical infrastructure sectors.

Important Dates

Monthly Test - 3rd Monday of each month

CWIN Program Management Office

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: cwin@dhs.gov
Web: www.ncs.gov

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
National Communications System
P.O. Box 4502
Arlington, VA 22204-4502

24/7 Help Desk:
1-877- 441-9330

Technical Support: Service Management Center (SMC)

VoIP Phone Ext: 4357 (HELP)
Tel: 1-877-441-9330 (Toll Free)
E-mail: smc@arrowhead.com
CWIN E-mail: ncc.help